Contents

1. What Is This Project?
2. Ubiquitous Normalization Of Data Collection
3. Configuring AME For Stable And Secure Operation
    1. Windows Update And Security Concerns
    2. The Case For Our Method
4. How do I enable the built-in SSH/SFTP server?
5. How do I change the username/password?
6. Is there a way to change the keyboard language in AME?
7. How do I enable the dark theme?
8. Why the old windows build?
9. Can AME be activated with a legit key, like normal Windows?
10. Is DirectX 12 supported?
11. Legal Considerations
12. Privacy or Security?
    1. Windows Updates
    2. Open Source
13. How do I enable Windows Script Host access?
14. How to add my user back to the Administrator group?
15. Why don't we base AME on LTS(B,C) releases?

What Is This Project?

Windows 10 AME aims at delivering a stable, non-intrusive yet fully functional build of Windows 10 to anyone, who requires the Windows operating system natively. Spyware systems, which are abundant in Windows 10 by default, have **not** been disabled using group policy, registry entries or various other workarounds – they have been entirely removed and deleted from the system, on an executable-level. This includes Windows Update, and any related services intended to re-patch the system via what is essentially a universal backdoor. Core applications, such as the included Edge web-browser, Windows Media Player, Cortana, as well as any appx applications, have also been successfully eliminated. The total size of removed files is about 2 GB.

Great effort has been invested in maintaining the subsequent system's stability, bug-free operation and user experience, as many of these removed services conflict with core Windows 10 features.

The Release Of Windows 10

When Microsoft released Windows 10 on July 29th 2015, it solidified its position in providing an operating system which undermined basic human rights with respect to privacy and overall system control. A shift towards an unjust source of power, via Windows Update and various other subsystems, amalgamated in a poorly designed user interface focused on cognitive ease and commercial advertising: This was to become the new era of computing. It's important to remark, that due to Windows 10's update mechanics, combined with Microsoft's decision of abolishing its testing devision for update distribution, a stock system is extremely unpredictable and subject to an ever-shifting, uncontrollable state of disarray - but nevertheless vulnerable to leaked back-doors, in cooperation with the NSA - seriously undermining and questioning the validity of the official narrative's claim to security and progress.

[SOURCE — www.eff.org] [SOURCE — autoriteitpersoonsgegevens.nl]

> *"[…] this program is an instrument of unjust power…. Sometimes it tracks the user... and sometimes they can even forcibly change the software at a distance, as Microsoft can with Windows, through the universal backdoor."* **– Richard M. Stallman, at TEDxGeneva 2014**

Configuring AME For Stable And Secure Operation

Due to the modified nature of this Windows installation, there are various possible security and stability concerns to consider when using Windows 10 AME. The entire removal of the Windows 10 update subsystem, coupled with the lack of automatic driver detection, beyond what is included in the ~~1511~~ 1809 build of Windows 10 from ~~November 2015~~ late 2018, requires manual action in order to configure proper and safe operation.

It is critical to understand, that Windows, regardless of its modernity and patched state, has proven to not be a secure platform. If security is one of your primary concerns, you should not be using AME, or Windows in general.

[SOURCE — www.schneier.com] [SOURCE — www.pcworld.com]

Windows Update And Security Concerns

Since the release of Windows 10, various security patches have been pushed to fix critical vulnerabilities, via Windows update distribution. These patches are not available for AME, as this subsystem has been disabled. In order to secure the system properly, it is strongly advised to revoke administrator privileges from the default user. This will mediate approximately 94% of the critical attack surface, while locking down the system from most foreseeable major future threats.

[SOURCE — www.avecto.com] [SOURCE — www.tenforums.com]

The use of networked Windows file-sharing using the SMB protocol, which, since the release of build 1511, has been hijacked for various large-scale exploits, such as the famed WannaCry ransomware attack, yet still showing extensive vulnerabilities, surfacing even today, should only be used in a user controlled, secured network environment, as this protocol has proven to be largely apprehensive by age of its design. SFTP is strongly recommended for networked file transfers.

[SOURCE — blogs.technet.microsoft.com]

The Case For Our Method

> *"[…] As you can see, even the recommended method for eliminating data collection isn't completely effective and causes a number of problems […] don't install anything, and don't use your computer, the data sent to Microsoft is quite minimal."* **– Mark Burnett, xato.net, May 2017**

In May 2017 a security researcher named Mark Burnett demonstrated that disabling the default data collection toggles, found in Windows 10's settings app, are entirely useless. Furthermore he showed that even through using intensive group policy modifications, in a process heavily scrutinized and iterated upon over several days, he was not able to prevent Windows 10 from sending critical, personally identifiable information with certainty.

[SOURCE — xato.net] [SOURCE — www.theinquirer.net]

In conclusion, it appears to be extremely difficult to genuinely disable data collection, as proven to be monitorable in a controlled environment, where a constant uncertainty, subject to change by Microsoft's backdoor via Windows Update, plagues any methodology of mitigation, when making use of the built-in tools of Windows 10 such as the basic Privacy settings, gpedit modifications or registry edits. The only logical and unfortunately required method in this scenario, is the removal of the affected services from the system entirely, along with Windows Update.

How do I enable the built-in SSH/SFTP server?

As discussed in the documentation, AME comes with the official SSH server installed by default, but has not been enabled due to concerns regarding the generated keys and opened ports.

To enable the server, first open the `firewall` rules for `sshd.exe` and allow inbound connections. Type the following into an elevated `powershell` prompt:

```
C:\> New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)' -
Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22
```

Start `sshd` (this will automatically generate host keys under `%programdata%\ssh` if they don't already exist):

```
C:\> net start sshd
```

The `sshd` service should also be configured to auto-start at boot. In an elevated powershell window type:

```
C:\> Set-Service sshd - StartupType Automatic
```

How do I change the username/password?

You can change the username in Windows from CMD (Administrator) using the following command:

```
C:\> wmic useraccount where name='currentname' rename newname
```

You can change a user's password in Windows from CMD (Administrator) using the following command:

```
C:\> net user useraccount *
```

Is there a way to change the keyboard language in AME?

Yes, the following changes the keyboard locale:

Open a Windows `powershell` prompt with Administrator rights.
Import the international settings module by running the following command:

```
C:\> ipmo international
```

Display the locale information on the computer by running the following command:

```
C:\> Get-WinSystemLocale
```

Set the locale for the region and language that you want. For example, the following command sets the system locale to German (Germany):

```
C:\> Set-WinUserLanguageList -Force 'de-DE'
```

How do I enable the dark theme?

The vanilla dark theme, while available, is not recommended, as it is extremely early in development. You can install a custom dark theme, however this appears to introduce a 15 second hang when logging in for some reason.

Why the old windows build? Old!

> This information only applies to prior AME releases, which were based on build 1511. Newer versions are much more up to date.

Multiple reasons, some having to do with the fact that MS added a whole other layer of complexity when trying to "ameliorate" versions past 1511.

However, this version is nearly "complete", and we will move on to 17.09 or 18.03, while also providing the older version, which will support older hardware longer, which MS will inevitably start to phase out support for at some point.

Can AME be activated with a legit key, like normal Windows?

No, the activation components are part of the *spyware aparatus*, and have been removed to the extent, that they don't send or collect personal data.

AME has been activated with a generic volume license key for Windows 10 Pro N RTM, and will never bother you to be activated, as it cannot verify the key with MS servers.

No *crackware* was employed to make windows think that it is activated, only the clever removal of components, in the right order.

> If you purchased your key from a third party, you may want to activate the key using a vanilla Windows 10 Installation on your machine before proceeding with AME, as the key will be tied to your motherboard and unable to be used again. Third party sellers sometimes check for this so they can make more money if you did not use the key within a short time period.

Is DirectX 12 Supported?

The general answer is no, as DirectX 12 is primarily updated by Windows Update, certain games will make API calls that aren't available on AME, resulting in crashes.

It is worth noting however, that due to DX12's proprietary nature, and Windows exclusivity, not to mention the fact that games, which make use of it, generally see no benefit at this point what so ever, it is advisable to avoid supporting the use of this API. There are promising open alternatives, such as Vulkan, as used by DOOM. Vulkan is **fully supported** by AME.

Legal Considerations

By downloading any of these images, you agree to Microsoft’s Terms of Service with respect to (5.) Authorized Software and Activation. All Images have been rudimentarily activated using a Generic Key for Windows 10 Pro N RTM. By using any of these images you agree that you have obtained a genuine product key or are able to activate by an other authorized method.

AME is developed for educational purposes only, which emphasizes an effort to reverse engineer, disable or replace components of the Microsoft Windows 10 operating system. The goal is an endeavor to better understand and mitigate the collection of Personally identifiable information (PII), as has been clearly outlined by numerous outlets covering the topic, including comments by famed whistle-blower Edward Snowden. Another goal is to replace included proprietary Windows software, such as the Edge web-browser, with ethically verifiable alternatives using open-source licenses.

[SOURCE — www.eff.org]

EU Directive 2009/24, on the legal protection of computer programs, governs reverse engineering in the European Union. The directive states:

"(15) The unauthorised reproduction, translation, adaptation or transformation of the form of the code in which a copy of a computer program has been made available constitutes an infringement of the exclusive rights of the author. ***Nevertheless****, circumstances may exist when such a reproduction of the code and translation of its form are indispensable to obtain the necessary information to achieve the* ***interoperability*** *of an independently created program with other programs. It has therefore to be considered that, in these limited circumstances only, performance of the acts of reproduction and translation by or on behalf of a person having a right to use a copy of the program is legitimate and compatible with fair practice and must therefore be deemed not to require the authorisation of the rightholder. An objective of this exception is to make it possible to connect all components of a computer system, including those of different manufacturers, so that they can work together. Such an exception to the author's exclusive rights may not be used in a way which prejudices the legitimate interests of the rightholder or which conflicts with a normal exploitation of the program."*

[SOURCE — eur-lex.europa.eu]

The intentions as self-described by the AME project, clearly fall under the case-scenario of enabling better "interoperability", as the prevalence of proprietary software bundled with the Windows 10 operating system does not constitute an open standard in this regard.

Privacy or Security?

As stated on the main page, the objective of this project *“[…] aims at delivering a stable, non-intrusive yet fully functional build of Windows 10 to anyone, who requires the Windows operating system natively”*, while *“Spyware systems […] have been entirely removed and deleted from the system.”*

This is crucial to understand, as we do not provide a heightened state of security as the project’s main focus, beyond what is indirectly affected by the AME alterations. This does include many aspects likely to improve security, such as the reduction of many internal services and features, liable to third party vulnerability escalation (i.e. SMBv1, Edge, Wifi-Sense and many others), however these are, in fact, somewhat unintended side-effects of our, arguably somewhat ideologically fueled, removal process.

[SOURCE — blogs.technet.microsoft.com] [SOURCE — www.extremetech.com]

Furthermore, as touched upon on the main page, 94% of critical Windows 10 vulnerabilities can be mitigated by revoking administrator privileges from the default user. This is also an included feature in AME, and can be set-up by means of the initialization script, as this mode of operation is strongly encouraged.

[SOURCE — www.avecto.com] [SOURCE — www.tenforums.com]

The Deal With Updates

However, AME does not allow for the installation of critical security patches, by means of regular Windows Updates, as this subsystem has been stripped from the OS entirely. **Unfortunately, due to Windows 10’s background restoration behavior, it was deemed necessary to also remove any ability of manually**

installing update packages, as the system components required for this, are the same ones responsible for the entire Windows Update subsystem to begin with – it was all or nothing.

Additionally, manually patching the OS, if this were possible, considering the goals and values AME deploys, in fact installs and alters many unwanted components, partially restoring Windows 10’s spyware apparatus. Because of this, each patch requires a scrutinous re-evaluation of the OS, followed by additions to the removal and cleansing process.

Nevertheless, each release of AME has been patched up until its release version date.

Open Source

The creation of AME is led by individuals principally interested in the open flow of information, and equal distribution of knowledge, hence a strong inclination towards supporting free and open source software, or even activist efforts, such as the FSF’s ethics.
As of such, the replacement applications provided in AME also attempt to fall in line with open source considerations.
We by all means strongly encourage users unfamiliar with these concepts to explore them in detail, as they are much further reaching in their implications, than simply superficial effects on software development.

How do I enable Windows Script Host access?

As described in the documentation, AME ships with various modifications aiming at locking Windows down to a much more secure state. As part of this process hardentools disables a Windows feature called Script Host access. However, this feature is often required for doing development work with, for example, Visual Studio, which will error-out during the installation process, due to this feature missing. To re-enable Script Host access, open an elevated command promt and type the following command:

```
C:\> reg add "HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings" /v Enabled /t REG_DWORD /d 1 /f
```

After that, reboot your computer, and the relevant programs should now be able to make use of this feature.

You revert these changes by typing the following command:

```
C:\> reg add "HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings" /v Enabled /t REG_DWORD /d 0 /f
```

How to add my user back to the Administrator group?

Due to severe security considerations, the default user in AME has been revoked Administrator privileges. However, in certain situations this may cause potential issues, as Windows was not designed to operate in this state, per se. If you require administrator priviliges, you can add your user back to this group using the following command in an elevated command prompt:

> Note that while certain inconveniences may arise due to not having direct administrator privileges, we strongly recommend sticking with the configuration we ship, for security reasons.

```
C:\> net localgroup administrators user /add
```

After this, restart Windows, and the default user will have administrator privileges.

Why don't we base AME on LTS(B,C) releases?

Windows 10 LTS releases, such as LTSB, which is based on build 1511, or LTSC, which is based on build 1809, have limited longevity with respect to hardware and driver support. This makes sense, given that the entire goal of the LTS Windows releases is to not change for multiple years. If we based AME on an LTS release, we would essentially only have one release, and then nothing for years on end. By basing AME on the Windows 10 Pro mainline releases, we have the ability to quickly respond, if software or driver incompatibilities emerge, due to the obsolescence of any specific build, as mainline releases are published about every six months by Microsoft.

[SOURCE — techcommunity.microsoft.net]